Ex. F - Claim Chart
U.S. Patent No. 10,503,418

US010503418B2

(12) **United States Patent**
Safa

(10) **Patent No.: US 10,503,418 B2**
(45) **Date of Patent: *Dec. 10, 2019**

(54) **SYSTEM AND METHOD TO SECURE A COMPUTER SYSTEM BY SELECTIVE CONTROL OF WRITE ACCESS TO A DATA STORAGE MEDIUM**

(71) Applicant: **Drive Sentry Limited**, Berkshire (GB)

(72) Inventor: **John Safa**, London (GB)

(73) Assignee: **Drive Sentry Limited** (GB)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **15/421,984**

(22) Filed: **Feb. 1, 2017**

(65) **Prior Publication Data**

US 2017/0147245 A1 May 25, 2017

Related U.S. Application Data

(63) Continuation-in-part of application No. 11/858,752, filed on Sep. 20, 2007, now Pat. No. 7,664,924, and
(Continued)

(51) **Int. Cl.**
G06F 3/06 (2006.01)
H04L 29/06 (2006.01)
(Continued)

(52) **U.S. Cl.**
CPC ***G06F 3/0622*** (2013.01); ***G06F 3/0659*** (2013.01); ***G06F 3/0676*** (2013.01);
(Continued)

(58) **Field of Classification Search**
CPC G06F 3/0622; G06F 3/0643; G06F 3/0659; G06F 3/067; G06F 21/52; G06F 21/554;
(Continued)

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,410,700 A 4/1995 Fecteau et al.
5,778,432 A 7/1998 Rubin et al.
(Continued)

FOREIGN PATENT DOCUMENTS

GB 2402515 A 12/2004
JP 08044630 A 2/1996
(Continued)

OTHER PUBLICATIONS

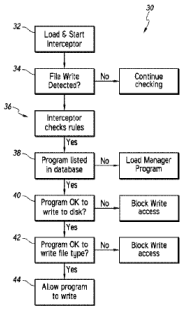
Dekart. Dekart Private Disk 2.06-Protect you data application by application. [online], [retrieved on Oct. 18, 2012]. Retrieved from the Internet.
(Continued)

Primary Examiner — Larry T Mackall
(74) *Attorney, Agent, or Firm* — Sabety + associates, PLLC; Ted Sabety

(57) **ABSTRACT**

A system and method of securing a computer system by controlling write access to a storage medium by monitoring an application; detecting an attempt by the application to write data to said storage medium; interrogating a rules database in response to said detection; and permitting or denying write access to the storage medium by the application in dependence on said interrogation.

32 Claims, 3 Drawing Sheets



Ex. F – Claim Chart
U.S. Patent No. 10,503,418

CLAIM 29	TREND MICRO PRODUCTS
29[pre] A method of controlling write access to a data storage device by an application running in application space on a first computer comprising:	Trend Micro performs the method of claim 29 via its Smart Protection Network. Specifically, Trend Micro offers many applications that can run on end-user devices (i.e., on a first computer) to protect those devices from electronic threats such as viruses, ransomware, malware, and the like (collectively "hostile applications"). That software includes but is not limited to, OfficeScan, Endpoint Application Control, Apex One, Antivirus+ Security, Internet Security, and Maximum Security. All of Trend Micro's software use the Smart Protection Network, which practices a method of controlling write access to a data storage device by an application running in application space on a first computer comprising as shown in this chart.

Trend Micro™

SMART PROTECTION NETWORK™

High performance global threat intelligence for your connected world

The Trend Micro™ Smart Protection Network™ continuously monitors and collects threat data from across the globe. We employ advanced detection analytics to immediately stamp out attacks before they can harm you. And the same accelerated cloud security powers all of our products and services, protecting millions of businesses and users around the globe.

Our threat researchers and data scientists use the latest techniques to analyze data and identify threats in real time. This is achieved through augmented cyber intelligence—which combines the focused findings from artificial intelligence (AI) and machine learning with knowledge from threat experts who are constantly researching the latest tactics, techniques, and procedures (TTPs) used by cybercriminals. We rapidly and accurately collate this wealth of global threat intelligence using automated security analytics to customize protection against the threats that are most likely to impact you.

To maintain this immense scale of threat protection, we've created one of the world's most extensive cloud-based infrastructures, delivering automatic correlation of threats across multiple security layers for customized protection, giving you threat visibility across platforms, security layers, and users globally. The Smart Protection Network, powered by XGen™, is an integral part of a connected threat defense, enabling Trend Micro products to use a cross-generational blend of threat defense techniques to stop threats as they are discovered.

HOW IT WORKS

The Smart Protection Network is segmented into three distinct areas: collection, identification, and protection.

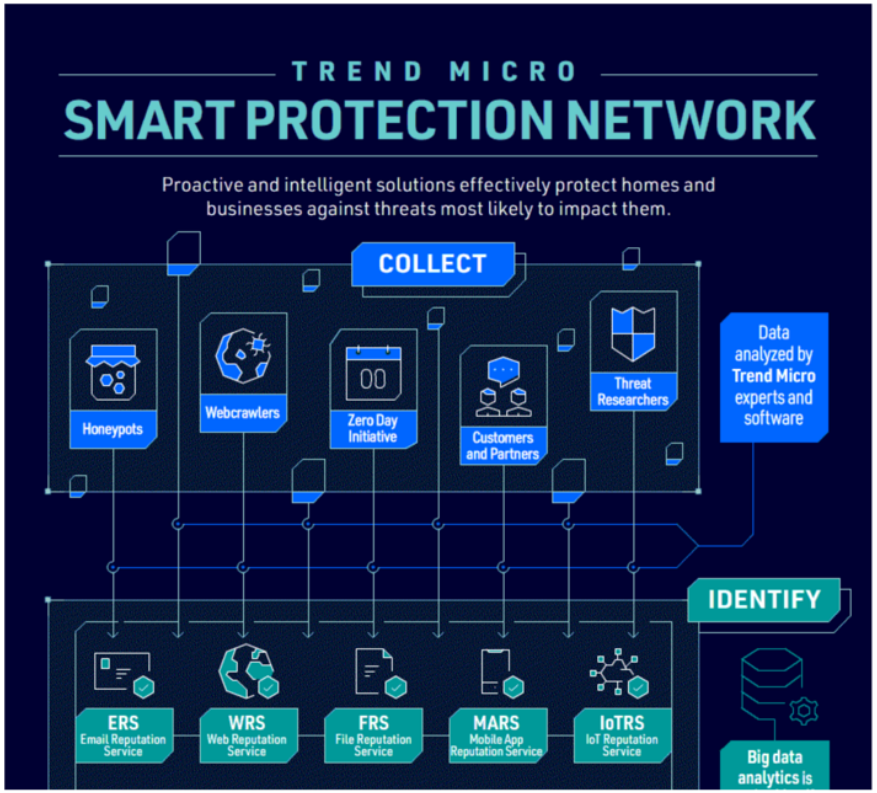
BY THE NUMBERS

The Trend Micro Smart Protection Network:

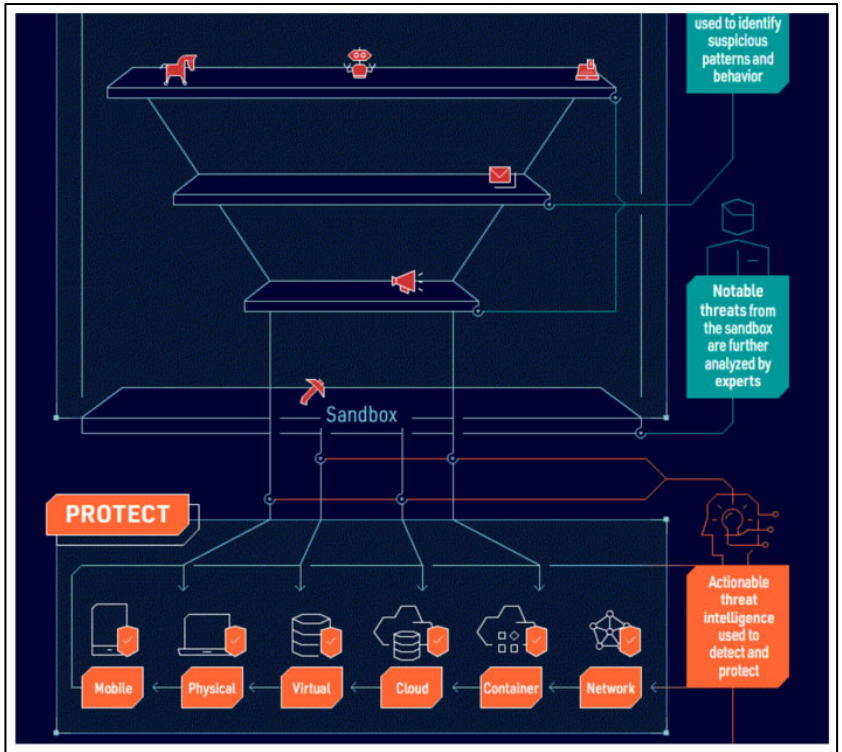
- Receives trillions of threat queries per year
- Analyzes 100s of terabytes of threat data per day
- Identifies billions of new, unique threats yearly
- Blocks 100s of millions of threats targeting our customers daily
- Has over 250 million sensors around the world
- Protects more than 500,000 businesses and millions of consumers globally
- Is powered by Trend Micro Research, with 450+ internal threat researchers and data scientists at 15 research centers around the world, and over 3,500 external white hat researchers supporting our bug bounty program, the Zero Day Initiative™

Datasheet, Trend Micro Smart Protection Network, at 1

Ex. F – Claim Chart
U.S. Patent No. 10,503,418

CLAIM 29	TREND MICRO PRODUCTS
29[a] receiving at a server computer from a plurality second computers operatively connected to the server by means of a data network, a corresponding plurality of permission values associated with the application operating on the first computer;	Trend Micro's Smart Protection Network receives at a server computer from a plurality second computers operatively connected to the server by means of a data network, a corresponding plurality of permission values associated with the application operating on the first computer. Trend Micro's Smart Protection Network includes servers that collect data via a data network from many resources that comprise a plurality of second computers, including from honeypots, webcrawlers, zero day initiative, customers and partners, and threat researchers.  https://www.trendmicro.com/en_us/business/technologies/smart-protection-network.html

Ex. F – Claim Chart
U.S. Patent No. 10,503,418

CLAIM 29	TREND MICRO PRODUCTS
29[a] receiving at a server computer from a plurality second computers operatively connected to the server by means of a data network, a corresponding plurality of permission values associated with the application operating on the first computer;	Trend Micro's Smart Protection Network servers also collect data from a plurality of second computers, including from its sandbox. Those servers receive a corresponding plurality of permission values associated with the application running on the first computer from the computers of the honeypots, webcrawlers, zero day initiative, customers and partners, threat researchers, and sandbox. Those permission values can be, for example, allowing the application access, denying the application access, a trusted program value, a whitelist value, a blacklist value, a blocked program value, or an allowed program value.  https://www.trendmicro.com/en_us/business/technologies/smart-protection-network.html

Ex. F – Claim Chart
U.S. Patent No. 10,503,418

CLAIM 29	TREND MICRO PRODUCTS
29[b] storing said permission values;	Trend Micro's Smart Protection Network stores the permission values so that it can accurately update its overall threat database using all its available resources. COLLECT IN VOLUME The Smart Protection Network collects terabytes of threat data every day through a global network of honeypots, submissions, feedback loops, and web-crawling technologies. We combine this data with insights from customers, partners, and our own threat researchers to provide greater visibility into the nature of attacks. The collected data includes an ever-growing volume of threat vectors, including threats associated with URLs, IPs, domains, files, exploits and vulnerabilities, network traffic, command and control, cybercriminal undergrounds, threat toolkits and techniques, and mobile apps. With threat actors located in every corner of the world, and billions of new, unique threats emerging each year, only the Smart Protection Network is designed to collect the massive volume of data needed to discover and protect from the ever-increasing flow of attacks. Datasheet, Trend Micro Smart Protection Network, at 1

Ex. F – Claim Chart
U.S. Patent No. 10,503,418

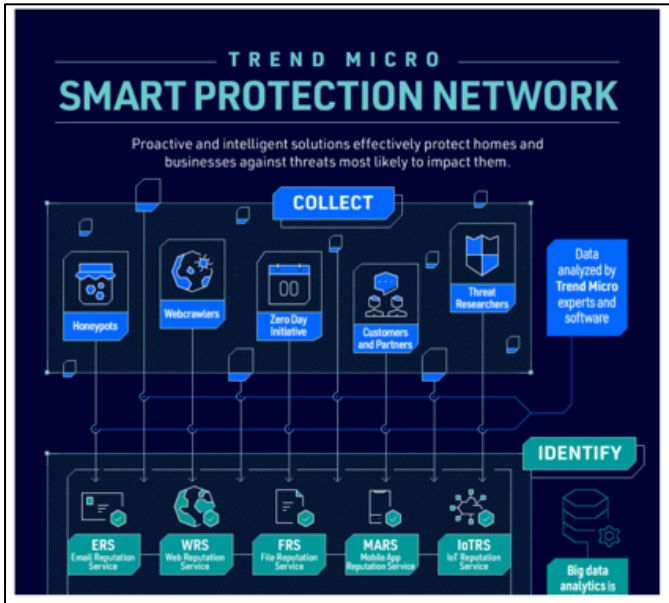
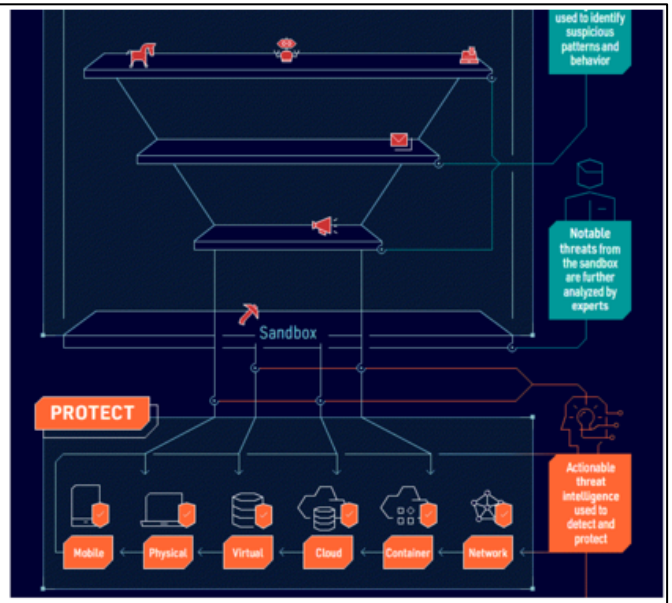
CLAIM 29	TREND MICRO PRODUCTS
29[c] generating an output permission value for the application in dependence on the stored permission values;	Trend Micro's Smart Protection Network generates an output permission value for the application in dependence on the stored permission values. For example, if the stored permission values indicate that a hostile application was allowed access to a computer, resulting in a threat detection, an output permission value to reject access for that application will be generated and updated to Trend Micro's customers using the Smart Protection Network. An important function of the Smart Protection Network is its ability to learn from its former actions: patterns of newly identified threats are maintained (sometimes for years) in the growing dataset of the Smart Protection Network for use in the future (i.e. retrospective analysis). Trends associated with customer type, geolocation, industry, and other metadata are identified and included in this historical information. In addition, any threats detected at installed Trend Micro customer sites are immediately forwarded to the Smart Protection Network, where they are compared to known threats and catalogued. All of this near-real-time, actionable intelligence is then distributed through the Trend Micro cloud to update all its solutions and services around the clock to its worldwide customer base. A Holistic, Proactive Framework for Identifying and Preventing Cyber Attacks at 8

Ex. F – Claim Chart
U.S. Patent No. 10,503,418

<table>
<tr><th>CLAIM 29</th><th>TREND MICRO PRODUCTS</th></tr>
<tr><td>29[c] generating an output permission value for the application in dependence on the stored permission values;</td><td>As another example, if the stored permission values indicate that a benign application was allowed access to a computer without harm, an output permission value to allow access to that application will be generated and updated to Trend Micro’s customers using the Smart Protection Network.

<table>
<tr><th>COMPONENT</th><th>BENEFIT DELIVERED THROUGH OUR PRODUCTS</th></tr>
<tr><td>Reputation Services</td><td>Email, web, file, and mobile app services check the reputation of these threat vectors to block spam/phishing, compromised websites, malicious files, and malicious mobile apps</td></tr>
<tr><td>Command and Control Communication</td><td>Quickly identifies botnet or targeted attack behaviors by identifying communications between targets and threat actors’ servers</td></tr>
<tr><td>Vulnerabilities and Exploits</td><td>Rapidly discovers and protects you against known and zero-day exploits by virtually patching newfound vulnerabilities</td></tr>
<tr><td>Whitelisting</td><td>Protects against false positives using in-the-cloud whitelists from one of the world’s largest threat research databases</td></tr>
<tr><td>Threat Actor Intelligence</td><td>Proactively protects against new threats using active research and investigation to identify new attack methods before they are used by cybercriminals</td></tr>
<tr><td>Big Data Analytics and Data Mining Correlation</td><td>Provides immediate and automatic protection from a multitude of threats by continuously updating and correlating massive amounts of global threat intelligence</td></tr>
<tr><td>Artificial Intelligence and Machine Learning</td><td>Proactive detection of 0-hour threats using advanced detection and protection capabilities. Trend Micro has been a pioneer in the use of AI/ML for over 13 years and utilize this in over 20 areas within our cybersecurity solutions</td></tr>
<tr><td>Smart Protection Server</td><td>Safeguards network bandwidth, endpoint efficiency, and privacy by performing web and file reputation queries directly to local servers, instead of the public cloud</td></tr>
<tr><td>Smart Feedback</td><td>Speeds protection by automatically updating Trend Micro’s global threat intelligence each time a new threat is identified on a single customer’s routine reputation check</td></tr>
</table>
Datasheet, Trend Micro Smart Protection Network, at 2</td></tr>
</table>

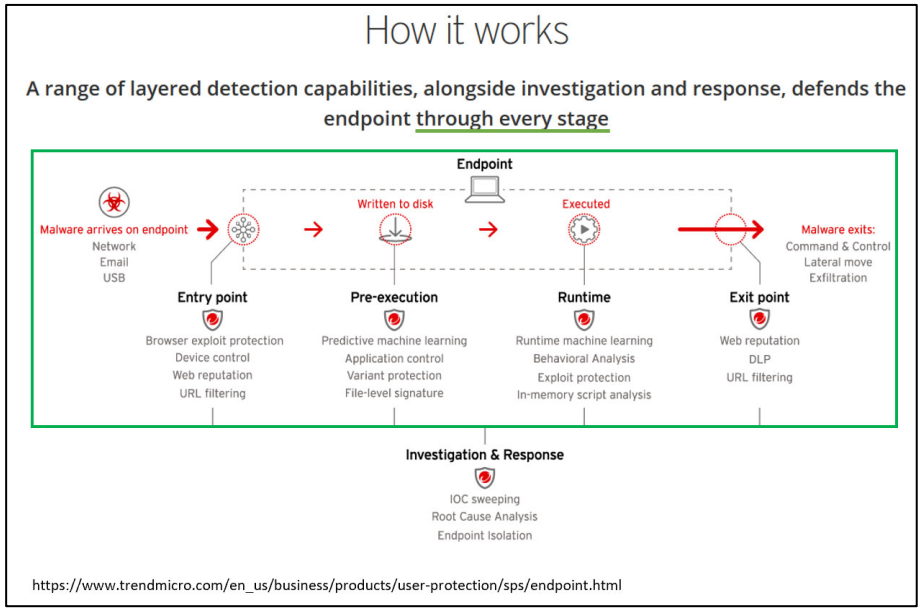
Ex. F – Claim Chart
U.S. Patent No. 10,503,418

CLAIM 29	TREND MICRO PRODUCTS
29[d] receiving at said server computer from the first computer operatively connected to the server by means of a data network, a request for a permission value associated with the application running on the first computer as a result of a process monitoring write access requests by the application on the first computer detecting an attempt by the application to write data to the data storage device, interrogating a local database of permission values and failing to locate a permission value associated with the application in the local database;	Trend Micro's Smart Protection Network servers receive said server computer from the first computer operatively connected to the server by means of a data network, a request for a permission value associated with the application running on the first computer as a result of a process monitoring write access requests by the application on the first computer detecting an attempt by the application to write data to the data storage device, interrogating a local database of permission values and failing to locate a permission value associated with the application in the local database. The computer using Trend Micro's software is operatively connected to Trend Micro's Smart Protection Network servers by means of a data network as shown below.   https://www.trendmicro.com/en_us/business/technologies/smart-protection-network.html

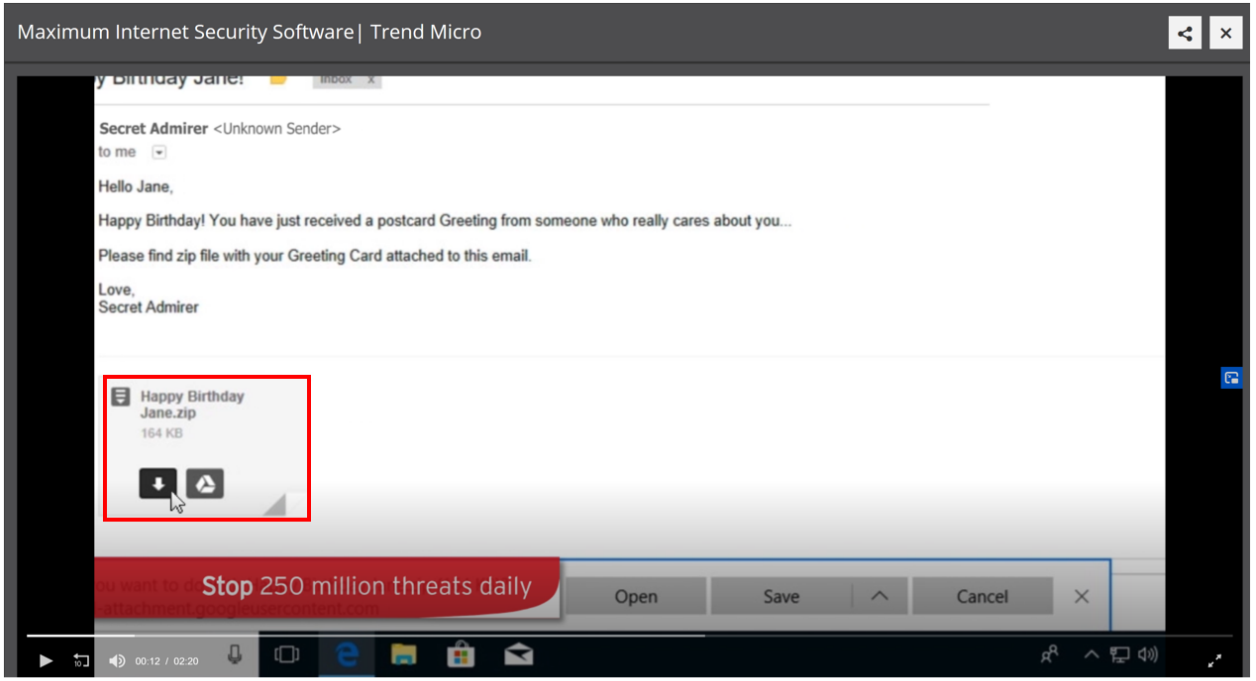
Ex. F – Claim Chart
U.S. Patent No. 10,503,418

CLAIM 29	TREND MICRO PRODUCTS
29[d] receiving at said server computer from the first computer operatively connected to the server by means of a data network, a request for a permission value associated with the application running on the first computer as a result of a process monitoring write access requests by the application on the first computer detecting an attempt by the application to write data to the data storage device, interrogating a local database of permission values and failing to locate a permission value associated with the application in the local database;	The computer using Trend Micro's software sends a threat query that is received at a server of Trend Micro's Smart Protection Network as a request for a permission value associated with the application running on the first computer. BY THE NUMBERS The Trend Micro Smart Protection Network: • Receives trillions of threat queries per year • Analyzes 100s of terabytes of threat data per day • Identifies billions of new, unique threats yearly • Blocks 100s of millions of threats targeting our customers daily • Has over 250 million sensors around the world • Protects more than 500,000 businesses and millions of consumers globally • Is powered by Trend Micro Research, with 450+ internal threat researchers and data scientists at 15 research centers around the world, and over 3,500 external white hat researchers supporting our bug bounty program, the Zero Day Initiative™ Datasheet, Trend Micro Smart Protection Network, at 1

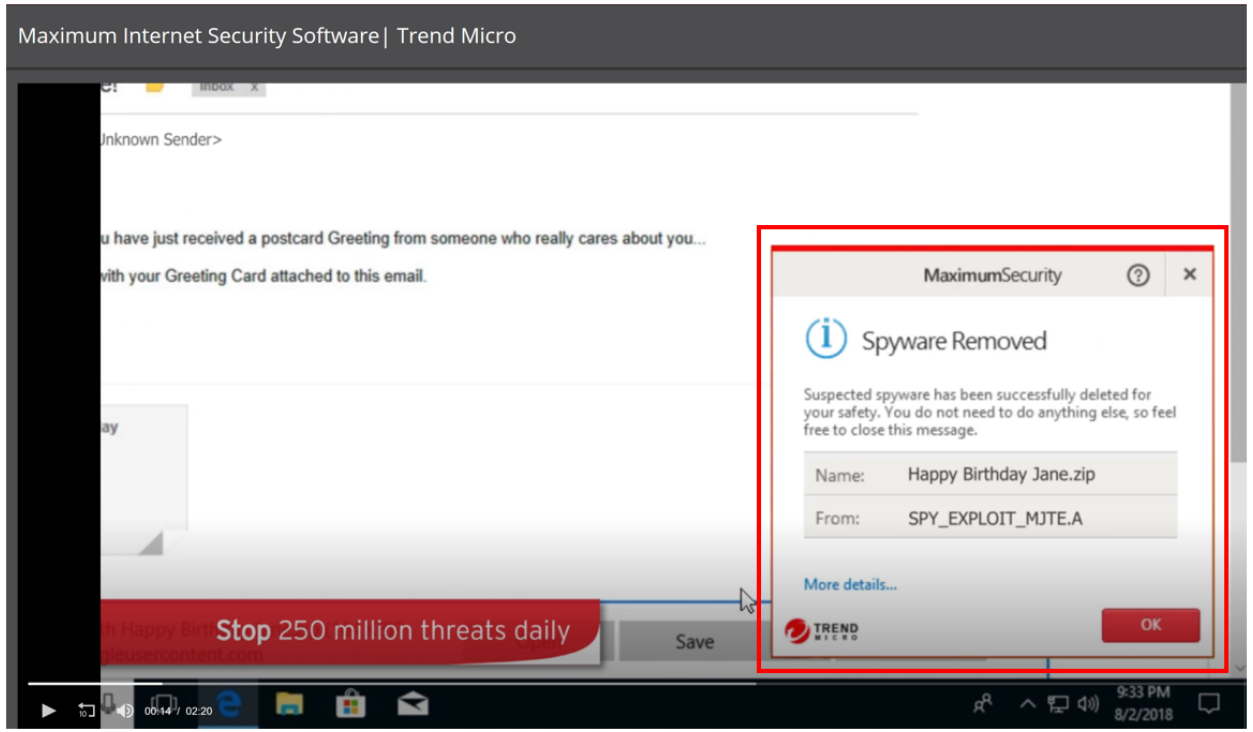
Ex. F – Claim Chart
U.S. Patent No. 10,503,418

CLAIM 29	TREND MICRO PRODUCTS
29[d] receiving at said server computer from the first computer operatively connected to the server by means of a data network, a request for a permission value associated with the application running on the first computer as a result of a process monitoring write access requests by the application on the first computer detecting an attempt by the application to write data to the data storage device, interrogating a local database of permission values and failing to locate a permission value associated with the application in the local database;	The computer using Trend Micro's software sends a threat query in response to that software monitoring write access requests attempts by the application and detecting an attempt by the application to write data to a storage device (e.g., hard drive or memory) on the computer. This attempt to write data can occur during every stage of the hostile application's presence: (1) entry-point; (2) pre-execution; (3) runtime; and (4) exit point. The graphic below showing how Trend Micro's software defends endpoints (e.g., the claimed "computer") is illustrative. First, when a hostile application arrives on an endpoint via for example a network, email, or USB, the software will detect attempts to write. Second, while a hostile application is being written to the storage medium, but before execution, the software detects the attempts to write. Third, while a hostile application is running it can make attempts to write data, which the software will detect. Fourth, when a hostile application exits it can make attempts to write data, which the software will also detect. 

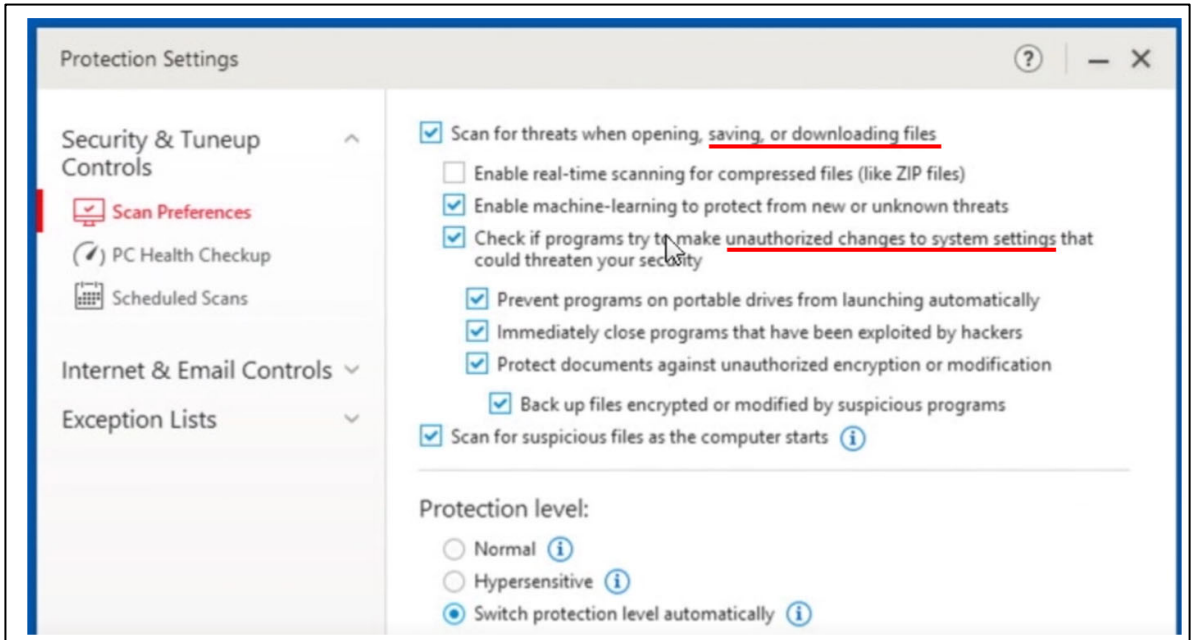
Ex. F – Claim Chart
U.S. Patent No. 10,503,418

CLAIM 29	TREND MICRO PRODUCTS
29[d] receiving at said server computer from the first computer operatively connected to the server by means of a data network, a request for a permission value associated with the application running on the first computer as a result of a process monitoring write access requests by the application on the first computer detecting an attempt by the application to write data to the data storage device, interrogating a local database of permission values and failing to locate a permission value associated with the application in the local database;	Trend Micro's software detects attempts by hostile applications to write data to a data storage device in any of the four stages outlined above. The example on this slide shows Trend Micro's Maximum Security detecting an attempt to write by an email attachment. In the image below, the user attempts to and or downloads a zip file from an email attachment, which would cause data to be written to the storage device. In the image on the next slide, Trend Micro's software detects that attempt to write.  https://www.trendmicro.com/en_us/forHome/products/maximum-security.html

Ex. F – Claim Chart
U.S. Patent No. 10,503,418

CLAIM 29	TREND MICRO PRODUCTS
29[d] receiving at said server computer from the first computer operatively connected to the server by means of a data network, a request for a permission value associated with the application running on the first computer as a result of a process monitoring write access requests by the application on the first computer detecting an attempt by the application to write data to the data storage device, interrogating a local database of permission values and failing to locate a permission value associated with the application in the local database;	The image below shows that Trend Micro's software detects that attempt to write before the user has clicked to save the file.  https://www.trendmicro.com/en_us/forHome/products/maximum-security.html

Ex. F – Claim Chart
U.S. Patent No. 10,503,418

CLAIM 29	TREND MICRO PRODUCTS
29[d] receiving at said server computer from the first computer operatively connected to the server by means of a data network, a request for a permission value associated with the application running on the first computer as a result of a process monitoring write access requests by the application on the first computer detecting an attempt by the application to write data to the data storage device, interrogating a local database of permission values and failing to locate a permission value associated with the application in the local database;	The image below shows another example of Trend Micro's Security software's ability to detect attempts by hostile applications to write data to a data storage device. As the image shows, the software scans for threats when saving or downloading files or when programs try to make unauthorized changes to system settings.  https://www.trendmicro.com/en_us/forHome/products/maximum-security.html 2. The following **Scan Preferences** are displayed. Check or uncheck to change a setting. • **Scan for threats when opening, saving, or downloading suspicious files.** This is the real-time scan that protects you at all times when you're using your computer. This is enabled by default. Trend Micro Security 2020 for Windows Product Guide at 72.

Ex. F – Claim Chart
U.S. Patent No. 10,503,418

CLAIM 29	TREND MICRO PRODUCTS
29[d] receiving at said server computer from the first computer operatively connected to the server by means of a data network, a request for a permission value associated with the application running on the first computer as a result of a process monitoring write access requests by the application on the first computer detecting an attempt by the application to write data to the data storage device, interrogating a local database of permission values and failing to locate a permission value associated with the application in the local database;	The image below shows another example of Trend Micro's Security software's ability to detect attempts by hostile applications to write data to a data storage device. As the image shows, threats are caught as they try to enter memory or touch the hard drive. **Quick Start: Conducting On-Demand Scans** By default, Trend Micro Security activates a **real-time scan** when it is installed. This is always present in memory, to proactively protect you from real-time threats. Threats are caught as they try to enter memory or touch the hard drive, preventing infections. This includes protection against ransomware, which may infect you from dangerous websites or emails. Trend Micro Security 2020 for Windows Product Guide at 60.

Ex. F – Claim Chart
U.S. Patent No. 10,503,418

CLAIM 29	TREND MICRO PRODUCTS
29[d] receiving at said server computer from the first computer operatively connected to the server by means of a data network, a request for a permission value associated with the application running on the first computer as a result of a process monitoring write access requests by the application on the first computer detecting an attempt by the application to write data to the data storage device, interrogating a local database of permission values and failing to locate a permission value associated with the application in the local database;	Trend Micro's Office Scan and Apex One software also include real-time scans, which detect attempts by hostile applications to write data to the computer's data storage device. **Real-time Scan: Advanced Settings** **Option** / **Description** **Scan Trigger** • **Read**: Scans files whose contents are read; files are read when they are opened, executed, copied, or moved. • **Write**: Scans files whose contents are being written; a file's contents are written when the file is modified, saved, downloaded, or copied from another location. • **Read or write** https://docs.trendmicro.com/all/ent/officescan/v11.0/en-us/osce_11.0_agent_olh/scn_adv_sttng_rltm_osce_agent.html (Office Scan Agent) **Real-time Scan** Real-time Scan is a persistent and ongoing scan. Each time a file is received, opened, downloaded, copied, or modified, Real-time Scan scans the file for security risks. If the Security Agent does not detect a security risk, users can proceed to access the file. If the Security Agent detects a security risk or a probable virus/malware, a notification message displays indicating the name of the infected file and the specific security risk. Real-time Scan maintains a persistent scan cache which reloads each time the Security Agent starts. The Security Agent tracks any changes to files or folders that occurred since the Security Agent unloaded and removes these files from the cache. Trend Micro Apex One Administrator's Guide at 7-14

Ex. F – Claim Chart
U.S. Patent No. 10,503,418

CLAIM 29	TREND MICRO PRODUCTS
29[d] receiving at said server computer from the first computer operatively connected to the server by means of a data network, a request for a permission value associated with the application running on the first computer as a result of a process monitoring write access requests by the application on the first computer detecting an attempt by the application to write data to the data storage device, interrogating a local database of permission values and failing to locate a permission value associated with the application in the local database;	Trend Micro's software also includes Behavior Monitoring that detects attempts by hostile applications to write data to a data storage device. As explained in the excerpt below, Behavior Monitoring constantly monitors endpoints, e.g., the claimed computers, for unusual modifications to the operating system or on installed software, e.g., attempts to write data to a data storage device. **Behavior Monitoring** Behavior Monitoring constantly monitors endpoints for unusual modifications to the operating system or on installed software. Behavior Monitoring protects endpoints through **Malware Behavior Blocking** and **Event Monitoring**. Complementing these two features are a user-configured **exception list** and the **Certified Safe Software Service**. Office Scan, Service Pack 1, Administrator's Guide at 9-2

Ex. F – Claim Chart
U.S. Patent No. 10,503,418

CLAIM 29	TREND MICRO PRODUCTS
29[d] receiving at said server computer from the first computer operatively connected to the server by means of a data network, a request for a permission value associated with the application running on the first computer as a result of a process monitoring write access requests by the application on the first computer detecting an attempt by the application to write data to the data storage device, interrogating a local database of permission values and failing to locate a permission value associated with the application in the local database;	The Behavior Monitoring service includes ransomware protection that detects attempts by applications to write data to a storage device of a computer. Those attempts to write occur, for example, in the attempts modify, delete, or rename files or in the modification of the file type.

OPTION	DESCRIPTION
Protect documents against unauthorized encryption or modification	You can configure Behavior Monitoring to detect a specific sequence of events that may indicate a ransomware attack. After Behavior Monitoring matches all of the following criteria, the OfficeScan agent terminates and attempts to quarantine malicious programs: 1. A process not recognized as safe attempts to modify, delete, or rename three files within a certain time interval. 2. The process attempted to modify a protected file extension type Additionally enable **Automatically back up files changed by suspicious programs** to create copies of files being encrypted on endpoints. After the encryption process completes and OfficeScan detects a ransomware threat, OfficeScan prompts end users to restore the affected files without suffering any loss of data. **Note** Automatic file backup requires at least 100 MB of disk space on the agent endpoint and only backs up files that are less than 10 MB in size. The backup folder location on agent endpoints is: <Agent installation folder>\CCSF\module\DRE\data. **WARNING!** If **Automatically back up files changed by suspicious programs** is not enabled, OfficeScan cannot recover the first files affected by a ransomware threat.

Office Scan, Service Pack 1, Administrator's Guide at 9-4

Ex. F – Claim Chart
U.S. Patent No. 10,503,418

CLAIM 29	TREND MICRO PRODUCTS
29[d] receiving at said server computer from the first computer operatively connected to the server by means of a data network, a request for a permission value associated with the application running on the first computer as a result of a process monitoring write access requests by the application on the first computer detecting an attempt by the application to write data to the data storage device, interrogating a local database of permission values and failing to locate a permission value associated with the application in the local database;	The following excerpt shows that Trend Micro's Security software (Antivirus+ Security, Internet Security, and Maximum Security) also include Behavior Monitoring functionality. **Trend Micro Security 2020 for Windows Product Guide** Trend Micro™ Antivirus+ Security Trend Micro™ Internet Security Trend Micro™ Maximum Security Trend Micro Security 2020 for Windows Product Guide at 1. **Unauthorized Change Prevention** Trend Micro Security includes behavior monitoring in its list of security protections. Unauthorized changes to system settings and other suspicious behavior can be blocked, as well as autorun programs on portable drives. Antivirus+ includes the ability to switch your protection level automatically, to aggressively eliminate programs that pose even a small risk of bad behavior. And the increased protection against ransomware that Folder Shield provides helps protect your computer and files from encryption or blocked access and the extortion that comes with ransomware. All editions of Trend Micro Security provide ransomware protection and Folder Shield. Trend Micro Security 2020 for Windows Product Guide at 70.

Ex. F – Claim Chart
U.S. Patent No. 10,503,418

CLAIM 29	TREND MICRO PRODUCTS
29[d] receiving at said server computer from the first computer operatively connected to the server by means of a data network, a request for a permission value associated with the application running on the first computer as a result of a process monitoring write access requests by the application on the first computer detecting an attempt by the application to write data to the data storage device, interrogating a local database of permission values and failing to locate a permission value associated with the application in the local database;	The following excerpt shows that Apex One also includes Behavior Monitoring functionality. **Behavior Monitoring** Behavior Monitoring constantly monitors endpoints for unusual modifications to the operating system or on installed software. Behavior Monitoring protects endpoints through **Malware Behavior Blocking** and **Event Monitoring**. Complementing these two features are a user-configured **exception list** and the **Certified Safe Software Service**. **Important** By default, Behavior Monitoring is disabled on all versions of Windows Server platforms. Trend Micro Apex One Administrator's Guide at 9-2

Ex. F – Claim Chart
U.S. Patent No. 10,503,418

CLAIM 29	TREND MICRO PRODUCTS
29[d] receiving at said server computer from the first computer operatively connected to the server by means of a data network, a request for a permission value associated with the application running on the first computer as a result of a process monitoring write access requests by the application on the first computer detecting an attempt by the application to write data to the data storage device, interrogating a local database of permission values and failing to locate a permission value associated with the application in the local database;	Trend Micro's Endpoint Application Control software also detects attempts by hostile applications to write data to a computer's data storage device. Endpoint Application Control detects those attempt to prevent them from occurring. For example it detects write attempts by executables, DDLs, Windows App store apps, device drivers, controls panels, and other portable executable files. Trend Micro Endpoint Application Control allows you to enhance your defenses against malware and targeted attacks by preventing unknown and unwanted applications from executing on your corporate endpoints. With a combination of flexible, dynamic policies, whitelisting and blacklisting capabilities, as well as an extensive application catalog, this easy-to-manage solution significantly reduces your endpoint attack exposure. For even greater insight into threats, user-based visibility and policy management are available in the local administration console or in the centrally-managed Trend Micro™ Control Manager™. Datasheet, Trend Micro Endpoint Application Control, at 1 Enhanced protection defends against malware, targeted attacks, and zero-day threats • Prevents potential damage from unwanted or unknown applications (executables, DLLs, Windows App store apps, device drivers, control panels, and other Portable Executable (PE) files) • Provides global and local real-time threat intelligence based on good file reputation data correlated across a global network Datasheet, Trend Micro Endpoint Application Control, at 1

Ex. F – Claim Chart
U.S. Patent No. 10,503,418

<table>
<tr><th>CLAIM 29</th><th>TREND MICRO PRODUCTS</th></tr>
<tr><td>29[d] receiving at said server computer from the first computer operatively connected to the server by means of a data network, a request for a permission value associated with the application running on the first computer as a result of a process monitoring write access requests by the application on the first computer detecting an attempt by the application to write data to the data storage device, interrogating a local database of permission values and failing to locate a permission value associated with the application in the local database;</td><td>Trend Micro’s software interrogates a local database of permission values to locate a permission value associated with the application in the local database. This includes interrogating databases populated by Trend Micro’s permission values or by permission values set by the user. Scans using the smart scan feature first interrogate a local database of permission values (“performs scanning on the local endpoint”). If it fails to locate a permission value associated with the application in the local database, it sends a scan query to the Smart Protection Network, and then caches the result of the scan query.
<table>
<tr><th>Basis of Comparison</th><th>Conventional Scan</th><th>Smart Scan</th></tr>
<tr><td>Scanning behavior</td><td>The conventional scan agent performs scanning on the local endpoint.</td><td>• The smart scan agent performs scanning on the local endpoint.
• If the agent cannot determine the risk of the file during the scan, the agent verifies the risk by sending a scan query to a smart protection source.
• The agent "caches" the scan query result to improve the scan performance.</td></tr>
<tr><td>Components in use and updated</td><td>All components available on the update source, except the Smart Scan Agent Pattern</td><td>All components available on the update source, except the Virus Pattern and Spyware Active-monitoring Pattern</td></tr>
<tr><td>Typical update source</td><td>OfficeScan server</td><td>OfficeScan server</td></tr>
</table>
Office Scan, Service Pack 1, Administrator’s Guide at 7-10</td></tr>
</table>

Ex. F – Claim Chart
U.S. Patent No. 10,503,418

<table>
<tr><th>CLAIM 29</th><th>TREND MICRO PRODUCTS</th></tr>
<tr><td>29[d] receiving at said server computer from the first computer operatively connected to the server by means of a data network, a request for a permission value associated with the application running on the first computer as a result of a process monitoring write access requests by the application on the first computer detecting an attempt by the application to write data to the data storage device, interrogating a local database of permission values and failing to locate a permission value associated with the application in the local database;</td><td>As another example, Apex One includes the same functionality as Office Scan’s functionality discussed on the previous slide.

TABLE 7-3. Conventional Scan and Smart Scan Compared
<table><tr><th>BASIS OF COMPARISON</th><th>CONVENTIONAL SCAN</th><th>SMART SCAN</th></tr><tr><td>Scanning behavior</td><td>The conventional scan Security Agent performs scanning on the local endpoint.</td><td>• The smart scan Security Agent performs scanning on the local endpoint.
• If the Security Agent cannot determine the risk of the file during the scan, the Security Agent verifies the risk by sending a scan query to a smart protection source.
• The Security Agent "caches" the scan query result to improve the scan performance.</td></tr></table>Trend Micro Apex One Administrator’s Guide at 7-9</td></tr>
</table>

Ex. F – Claim Chart
U.S. Patent No. 10,503,418

CLAIM 29	TREND MICRO PRODUCTS
29[d] receiving at said server computer from the first computer operatively connected to the server by means of a data network, a request for a permission value associated with the application running on the first computer as a result of a process monitoring write access requests by the application on the first computer detecting an attempt by the application to write data to the data storage device, interrogating a local database of permission values and failing to locate a permission value associated with the application in the local database;	Trend Micro's Security software also uses a local database of permission values in combination with the online database of the Smart Protection Network. The signature database is maintained "mainly on Trend Micro Servers in the cloud," which means that at least some of the database is stored locally. Unlike other local-protection-based products that require you to frequently update a large local signature database on your computer, Trend Micro Security updates the signature database mainly on Trend Micro Servers in the cloud, so all consumers of the Smart Protection Network are instantly protected whenever the online database is updated. Other cloud-based and local Trend Micro technologies correlate threat data of different kinds, since modern threats can simultaneously use multiple techniques to infect your computer. Smart Scan reduces network bandwidth usage (for updating/downloading signatures), while saving disk space and memory. Trend Micro Security 2020 for Windows Product Guide at 61.

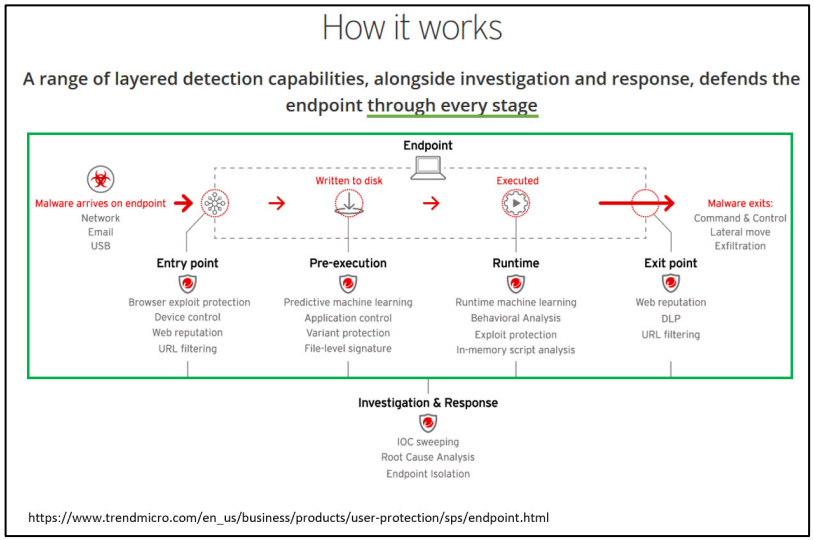
Ex. F – Claim Chart
U.S. Patent No. 10,503,418

CLAIM 29	TREND MICRO PRODUCTS
29[d] receiving at said server computer from the first computer operatively connected to the server by means of a data network, a request for a permission value associated with the application running on the first computer as a result of a process monitoring write access requests by the application on the first computer detecting an attempt by the application to write data to the data storage device, interrogating a local database of permission values and failing to locate a permission value associated with the application in the local database;	Office Scan also interrogates a local database of permission values from an exception list for approved programs and blocked programs. If a program is on the exception list as an approved program, Office Scan does not monitor that program. If a program is on the exception list as a blocked program, Office Scan blocks that program. Upon information and belief, the programs on the exception list are stored on a database that include data elements encoding permission values, e.g., approved or blocked, that are associated with the applications on the list. **Behavior Monitoring Exception List** The Behavior Monitoring exception list contains programs that the OfficeScan agent does not monitor using Behavior Monitoring. • **Approved Programs**: The OfficeScan agent allows all programs in the Approved Programs list to pass Behavior Monitoring scanning. **Note** Although Behavior Monitoring does not take action on programs added to the Approved Programs list, other scan features (such as file-based scanning) continue to scan the program before allowing the program to run. • **Blocked Programs**: The OfficeScan agent blocks all programs in the Blocked Programs list. To configure the Blocked Programs list, enable Event Monitoring. 9-9 Configure the exception list from the web console. You can also grant users the privilege to configure their own exception list from the OfficeScan agent console. For details, see *Behavior Monitoring Privileges on page 9-19*. Office Scan, Service Pack 1, Administrator's Guide at 9-9, 10.

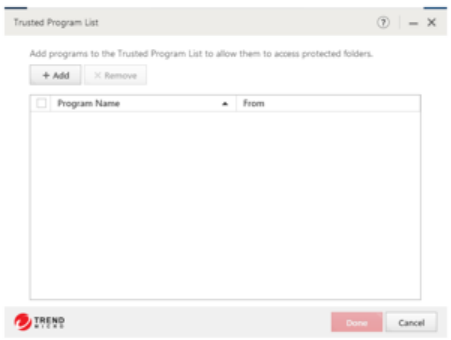
Ex. F – Claim Chart
U.S. Patent No. 10,503,418

CLAIM 29	TREND MICRO PRODUCTS
29[d] receiving at said server computer from the first computer operatively connected to the server by means of a data network, a request for a permission value associated with the application running on the first computer as a result of a process monitoring write access requests by the application on the first computer detecting an attempt by the application to write data to the data storage device, interrogating a local database of permission values and failing to locate a permission value associated with the application in the local database;	The Office Scan software also interrogates a local database of permission values from a Trusted Program list. Upon information and belief, the programs on that list are stored on a database that include data elements encoding permission values, e.g., trusted or not, that are associated with the applications on the list. **Trusted Program List** You can configure OfficeScan agents to skip scanning of trusted processes during Real-time and Behavior Monitoring scans. After adding a program to the Trusted Programs List, the OfficeScan agent does not subject the program or any processes initiated by the program to Real-time Scan. Add trusted programs to the Trusted Program List to improve the performance of scanning on endpoints. Office Scan, Service Pack 1, Administrator's Guide at 9-2

Ex. F – Claim Chart
U.S. Patent No. 10,503,418

CLAIM 29	TREND MICRO PRODUCTS
29[d] receiving at said server computer from the first computer operatively connected to the server by means of a data network, a request for a permission value associated with the application running on the first computer as a result of a process monitoring write access requests by the application on the first computer detecting an attempt by the application to write data to the data storage device, interrogating a local database of permission values and failing to locate a permission value associated with the application in the local database;	Office Scan interrogates a local database of permission values from a whitelist, such as the exception list and trusted programs lists at each layer or stage. • Progressively filters out threats using the most efficient technique for maximum detection without false positives. • Blends signature-less techniques including high-fidelity machine learning, behavioral analysis, variant protection, census check, application control, exploit prevention, and good-file check with other techniques like file reputation, web reputation, and command and control (C&C) blocking. • Trend Micro is the first to infuse high-fidelity machine learning which uniquely analyzes files not only before execution but also during runtime for more accurate detection. • Noise cancellation techniques like census and whitelist checking at each layer reduce false positives. • Instantly shares information on suspicious network activity and files with other security layers to stop subsequent attacks. • Advanced ransomware protection monitors for suspicious file encryption activities at the endpoint, terminates malicious activities, and even recovers lost files if necessary. Datasheet, Trend Micro Office Scan, at 2  https://www.trendmicro.com/en_us/business/products/user-protection/sps/endpoint.html

Ex. F – Claim Chart
U.S. Patent No. 10,503,418

CLAIM 29	TREND MICRO PRODUCTS
29[d] receiving at said server computer from the first computer operatively connected to the server by means of a data network, a request for a permission value associated with the application running on the first computer as a result of a process monitoring write access requests by the application on the first computer detecting an attempt by the application to write data to the data storage device, interrogating a local database of permission values and failing to locate a permission value associated with the application in the local database;	Trend Micro's other software packages also include exception lists and trusted programs list. The following excerpt shows that Antivirus+ Security, Internet Security, and Maximum Security also include exception lists / trusted program lists. **Exception Lists: Programs/Folders** **To add items to Exception Lists Programs/Folders:** Trend Micro Security lets you add programs, folders, or websites to exception lists so that scans will ignore them. Adding programs or folders to exception lists can increase performance during scans, while adding frequently-accessed websites can prevent unwanted blockage. Users are advised to use exception lists wisely, as it may open computers up to more threats. Trend Micro Security 2020 for Windows Product Guide at 84. 13. You can also click the link **Trusted Program List** to add a trusted program to a list of applications that can access protected folders. The **Trusted Program List** appears.  **Figure 193. Trusted Program List** Trend Micro Security 2020 for Windows Product Guide at 110-111.

Ex. F – Claim Chart
U.S. Patent No. 10,503,418

CLAIM 29	TREND MICRO PRODUCTS
29[d] receiving at said server computer from the first computer operatively connected to the server by means of a data network, a request for a permission value associated with the application running on the first computer as a result of a process monitoring write access requests by the application on the first computer detecting an attempt by the application to write data to the data storage device, interrogating a local database of permission values and failing to locate a permission value associated with the application in the local database;	The following excerpts also show that Apex One includes exception lists and trusted program lists. **Behavior Monitoring Exception List** The Behavior Monitoring exception list contains programs that the Security Agent does not monitor using Behavior Monitoring. • **Approved Programs**: The Security Agent allows all programs in the Approved Programs list to pass Behavior Monitoring scanning. Note Although Behavior Monitoring does not take action on programs added to the Approved Programs list, other scan features (such as file-based scanning) continue to scan the program before allowing the program to run. • **Blocked Programs**: The Security Agent blocks all programs in the Blocked Programs list. To configure the Blocked Programs list, enable Event Monitoring. Configure the exception list from the web console. You can also grant users the privilege to configure their own exception list from the Security Agent console. For details, see *Behavior Monitoring Privileges on page 9-18*. Trend Micro Apex One Administrator's Guide at 9-9 **Trusted Program List** You can configure Security Agents to skip scanning of trusted processes during Application Control, Behavior Monitoring, Data Loss Prevention, Device Control, Endpoint Sensor, and Real-time Scans. After adding a program to the Trusted Programs List, the Security Agent does not subject the program or any processes initiated by the program to Real-time Scan. Add trusted programs to the Trusted Program List to improve the performance of scanning on endpoints. Trend Micro Apex One Administrator's Guide at 7-51  Trend Micro Apex One™ Application Control™ • Prevents damage from unwanted/unknown applications (executables, DLLs, and other PE files). • Flexible, dynamic policies and whitelisting/blacklisting capabilities to reduce attack exposure. • Allows users to install applications based on reputation-based variables (prevalence, usage, and maturity). • Provides global and local real-time threat intelligence based on good file reputation data. • Categorizes applications and provides updates via our Trend Micro Certified Safe Software Service. • Coverage of pre-categorized applications that can be selected from our application catalog. • Visibility and policy management via Trend Micro Apex Central™. • Interconnects with additional layers of security to better correlate data and stop threats more often. Trend Micro Apex One Administrator's Guide at 9-9

Ex. F – Claim Chart
U.S. Patent No. 10,503,418

CLAIM 29	TREND MICRO PRODUCTS
29[d] receiving at said server computer from the first computer operatively connected to the server by means of a data network, a request for a permission value associated with the application running on the first computer as a result of a process monitoring write access requests by the application on the first computer detecting an attempt by the application to write data to the data storage device, interrogating a local database of permission values and failing to locate a permission value associated with the application in the local database;	The following excerpts also show that, during for example real-time scans that run in response to a write requests as discussed above, Office Scan and Apex One interrogating a local database of permission values. Those permission values are stored on a database containing the Smart Scan Agent Pattern on the computer. **Smart Scan Agent Pattern** The Smart Scan Agent Pattern is updated daily and is downloaded by the OfficeScan agents' update source (the OfficeScan server or a custom update source). The update source then deploys the pattern to smart scan agents. Note Smart scan agents are OfficeScan agents that administrators have configured to use File Reputation Services. Agents that do not use File Reputation Services are called conventional scan agents. Smart scan agents use the Smart Scan Agent Pattern when scanning for security risks. If the pattern cannot determine the risk of the file, another pattern, called Smart Scan Pattern, is leveraged. **Smart Scan Pattern** The Smart Scan Pattern is updated hourly and is downloaded by smart protection sources. Smart scan agents do not download the Smart Scan Pattern. Agents verify potential threats against the Smart Scan Pattern by sending scan queries to smart protection sources. Office Scan, Service Pack 1, Administrator's Guide at 4-8

Ex. F – Claim Chart
U.S. Patent No. 10,503,418

CLAIM 29	TREND MICRO PRODUCTS
29[d] receiving at said server computer from the first computer operatively connected to the server by means of a data network, a request for a permission value associated with the application running on the first computer as a result of a process monitoring write access requests by the application on the first computer detecting an attempt by the application to write data to the data storage device, interrogating a local database of permission values and failing to locate a permission value associated with the application in the local database;	The following excerpts shows the same Smart Scan Agent Pattern for the Apex One. **Smart Scan Agent Pattern** The Smart Scan Agent Pattern is updated daily and is downloaded by the Apex One agents' update source (the Apex One server or a custom update source). The update source then deploys the pattern to smart scan agents. **Note** Smart scan agents are Security Agents that administrators have configured to use File Reputation Services. Agents that do not use File Reputation Services are called conventional scan agents. Smart scan agents use the Smart Scan Agent Pattern when scanning for security risks. If the pattern cannot determine the risk of the file, another pattern, called Smart Scan Pattern, is leveraged. **Smart Scan Pattern** The Smart Scan Pattern is updated hourly and is downloaded by smart protection sources. Smart scan agents do not download the Smart Scan Pattern. Agents verify potential threats against the Smart Scan Pattern by sending scan queries to smart protection sources. Trend Micro Apex One Administrator's Guide at 4-8

Ex. F – Claim Chart
U.S. Patent No. 10,503,418

CLAIM 29	TREND MICRO PRODUCTS
29[d] receiving at said server computer from the first computer operatively connected to the server by means of a data network, a request for a permission value associated with the application running on the first computer as a result of a process monitoring write access requests by the application on the first computer detecting an attempt by the application to write data to the data storage device, interrogating a local database of permission values and failing to locate a permission value associated with the application in the local database;	As shown in the previous slides, the interrogation of the local database results in failure to locate a permission value, the Smart Protection Network receives a request for the permission value. BY THE NUMBERS The Trend Micro Smart Protection Network: • Receives trillions of threat queries per year • Analyzes 100s of terabytes of threat data per day • Identifies billions of new, unique threats yearly • Blocks 100s of millions of threats targeting our customers daily • Has over 250 million sensors around the world • Protects more than 500,000 businesses and millions of consumers globally • Is powered by Trend Micro Research, with 450+ internal threat researchers and data scientists at 15 research centers around the world, and over 3,500 external white hat researchers supporting our bug bounty program, the Zero Day Initiative™ Datasheet, Trend Micro Smart Protection Network, at 1

Ex. F – Claim Chart
U.S. Patent No. 10,503,418

CLAIM 29	TREND MICRO PRODUCTS
29[e] selecting the stored permission value in response to receiving the request; and **29[f] transmitting to said first computer the output permission value derived from the plurality of received permission values to the first computer over the data network in order to cause the monitoring process operating on the first computer to permit or deny write access by the application to the data storage device in dependence on the transmitted output permission value.**	For the Smart Protection Network to respond to a query or update a local signature database, it must select the stored permission value in response to receiving the request and transmit it to the first computer. The output permission value is derived from the plurality of received permission values as discussed for limitation 29[c]. That response is sent to cause the Trend Micro software operating on the first computer to permit or deny write access by the application to the data storage device in dependence on the transmitted output permission value. As discussed previously, the purpose of the Smart Protection Network is to provide Trend Micro's users with up-to-date information on whether applications are hostile. And as discussed previously, that information is used to determine whether to allow or deny write access to the application.